Chapter: Medical Records (MR)
Section 1: Medical Records Service

Policy

Utah State Hospital maintains medical records that are documented accurately and in a timely manner, are readily accessible, and permit prompt retrieval of information.

Procedure

1. A medical record is maintained for each individual who is evaluated or treated. Portions of the medical record are maintained in electronic format (E-Chart).

    1.1. E-Chart is considered the official record for all components that have been reviewed and authorized for use.

    1.2. As additional aspects of the medical record are designed, tested, and approved, E-Chart will be expanded.

2. The purposes of the medical record are as follows:

    2.1. to serve as a basis for planning patient care and for continuity in the evaluation of the patient's condition and treatment;

    2.2. to furnish documentary evidence of the course of the patient's medical evaluation, treatment, and change in condition during the hospital stay;

    2.3. to document communication between the practitioner responsible for the patient and any other health care professional who contributes to the patient's care;

    2.4. to assist in protecting the legal interest of the patient, the hospital, and the practitioner responsible for the patient;

    2.5. to provide data for use in continuing education and in research; and

    2.6. to document services provided in order to support reimbursement claims that are submitted to payers.

3. All significant clinical information pertaining to a patient is incorporated in the patient's medical record.

4. The content of the medical record is sufficiently detailed and organized to enable:

    4.1. the practitioner responsible for the patient to provide continuing care to the patient, determine later what the patient's condition was at a specific time, and review the diagnostic and therapeutic procedures performed and the patient's response to treatment;

    4.2. a consultant to render an opinion after an examination of the patient and a review of the medical record;

4.3. another practitioner to assume the care of the patient at any time; and

4.4. the retrieval of pertinent information required for utilization review and quality assessment and improvement activities.

5. The Medical Records Service is directed by a Registered Health Information Technician (RHIT).

6. A terminal digit filing system is used based on the patient's assigned hospital number for ease in retrieval of records.

7. To assure that the maximum possible information about a patient is available to the professional staff providing care, there is one electronic record, one working chart, and one permanent chart. A patient's medical record may be thinned as necessary. Minimum guidelines for documents kept in the working chart are available in Medical Records Department.

8. Pertinent medical information obtained on request from outside sources is filed with, but not necessarily as part of the patient's medical record. Such information is available to professional staff concerned with the care and treatment of the patient.

9. A standardized filing order for the working chart is used throughout the hospital and is available in Medical Records Department.

10. Patient records are maintained in paper and electronic format. Paper format is maintained on active shelves for five years following discharge. Paper charts are then pulled and placed in inactive storage until retention is met. Retention for patient records is seven (7) years after date of discharge for adults and/or age of majority plus four (4) years for children/youth records.

10.1. When retention is met, the following identified documents are extracted, if they exist in hard copy, and are imaged into electronic format:

10.1.1. Legal commitment papers/court orders;
10.1.2. Discharge summary and/or death summary
10.1.3. Initial psychiatric assessment;
10.1.4. Initial physical examination;
10.1.5. Initial social history assessment;
10.1.6. Initial nursing assessment;
10.1.7. Occupational therapy assessment;
10.1.8. Dental records;
10.1.9. Psychological assessment;
10.1.10. Neurological consultations;
10.1.11. Basic patient demographic information;
10.1.12. Treatment staff;
10.1.13. Diagnoses.
10.1.14. Discharge Order

10.2. After imaging is completed, extracted paper records are sent for permanent storage to Utah State Archives and the remainder of the record is destroyed.

10.3. When there are changes to technical platform of electronic records, imaged records will be included in upgrade to insure accessibility.

Implemented: 6-28-88
Revised: 11-29-90
Revised: 4-92
Revised: 2-93
Revised: 11-94
Revised: 12-98
Revised: 3-02
Revised: 1-05
Revised: 7-07
Revised: 5-09
Reviewed: 9-13

Chapter: Medical Records (MR)
Section 2: Content of Medical Records

Policy

The information management function provides for the definition, capture, analysis, transformation, transmission, and reporting of individual patient specific data/information related to the processes and/or outcomes of the patient's care.

Procedure

1. A medical record is initiated and maintained for every individual assessed or treated. The medical record incorporates information from subsequent contacts between the patient and the organization.

    1.1. Entries in medical records are made only by individuals authorized to do so as specified in organization and medical staff policies.

    1.2. Electronic entries are considered official when clinician has reviewed their entries and electronically signed or noted off using authorized Personal Identification Number (PIN).

2. The medical record contains sufficient information to identify the patient, support the diagnosis, justify the treatment, accurately document the course and result of treatment, and facilitate continuity of care among health care providers. Each record, in electronic or paper format, contains at least the following:

    2.1. The patient's name, address, date of birth, and the name of any legally authorized representative;

    2.2. The patient's legal status;

    2.3. Emergency care provided to the patient prior to arrival, if any;

    2.4. The reason(s) for admission or treatment;

    2.5. The record and findings of the patient's assessment;

    2.6. A statement of the conclusions or impressions drawn from the medical history and physical examination;

    2.7. The diagnosis or diagnostic impression;

    2.8. A printed face sheet with the complete provisional diagnoses and demographic information.

    2.9. The goals of treatment and the treatment plan;

    2.10. Evidence of known advance directives;

    2.11. Evidence of informed consent for procedures and treatments for which informed consent is required by organizational policy;

    2.12. Diagnostic and therapeutic orders, if any;

2.13. All diagnostic and therapeutic procedures and tests preformed and the results;

2.14. Progress notes made by the medical staff and other authorized individuals;

2.15. All reassessments, when necessary;

2.16. Clinical observations;

2.17. The response of the care provided;

2.18. Consultation reports;

2.19. Every medication ordered or prescribed for an inpatient;

2.20. Every dose of medication administered and any adverse drug reaction;

2.21. All relevant diagnoses established during the course of care;

2.22. Any referrals/communications made to external or internal care providers and to community agencies.

3. All significant clinical information pertaining to a patient is entered into the medical record as soon as possible after its occurrence.

4. Names of patients other than the one whose chart is being noted on are not used.

5. In the event of a power failure rendering the electronic system inoperable for an extensive period of time, noting and physicians orders can be completed by using the forms available under the “Power Failure” tab in the working chart.

5.1. If it becomes necessary to use these forms, they should then be filed in the appropriate sections of the record (progress note divider and physician order divider) and become part of the patient record.

5.2. If power failure occurs when completing the initial assessments, these should be completed on the worksheets. When eChart is restored the information should be input into the electronic patient record with the correct assessment date and time.

5.3. In the event of a prolonged interruption of computer service to the hospital, refer to Technology Services Policy; Section 7: Disaster Data Recovery.

6. Telephone orders of authorized individuals are accepted and transcribed by qualified personnel who are identified by title or category in the medical staff rules and regulations.

6.1. Telephone orders for medications are accepted only by personnel so designated in the medical staff rules and regulations and are authenticated by the prescribing practitioner within 30 days.

6.2. Orders are entered directly by the prescriber unless the prescriber does not have immediate access to materials necessary to initiate the order.

6.3. Telephone orders are immediately read back to the prescriber by the RN and are acknowledged by the prescriber.

6.3.1. Telephone orders are entered directly into e-chart on the hard copy chart by the receiving RN.

6.3.2. After the telephone order is recorded in the record, it is read back by the receiving RN to the prescriber and verified by the prescriber.

6.4. Telephone orders are entered directly into e-chart or the hard copy chart by the receiving RN.

6.5. After the telephone order is recorded in the record, it is read back by the receiving RN to the prescriber and verified by the prescriber.

7. Verbal communication of critical test results are repeated back to the person reporting the results and acknowledged for accuracy by the person reporting the results.

7.1. All results reported by telephone are considered critical test results.

8. Orders for medication are entered in e-chart.

9. All entries in medical records are dated, timed and authenticated; a method is established to identify the authors of entries.

9.1. Authentication may be by written signatures, initials, or electronic signature.

9.1.1. When initials are used, there must be a legend in the patient record to identify the initials.

10. Elements of patient record that are authorized for electronic use are not duplicated in hard copy and placed in patient's permanent file with the exception of the Integrated Assessment. Printing and filing of the Provisional Treatment Plan and Individual Comprehensive Treatment Plan (ICTP) are left to the discretion of the unit SMT.

11. At discharge from inpatient care, a clinical resume concisely summarizes the reason for hospitalization, the significant findings, the procedures performed and treatment rendered, the patient's condition on discharge, medication dispensed to or prescribed on discharge; community resources and any specific instructions given to the patient and/or family, as pertinent.

12. Medical records of discharged patients are completed within a time period specified in medical staff rules and regulations, not to exceed 30 days.

13. The organization uses a patient information system to routinely assemble all divergently located components when a patient is admitted to the hospital.

Implemented: 6-28-88 *Revised: 5-3-89* *Revised: 11-29-90* *Revised: 4-92* *Revised: 2-93* *Revised: 11-94* *Revised: 4-96* *Revised: 12-98* *Revised: 3-02* *Revised: 3-04* *Revised: 1-05* *Revised: 8-07* *Revised: 5-09* *Revised: 2-11* *Revised: 9-13* *Revised: 1-15*	

Chapter: Medical Records (MR)
Section 3: Quality of the Medical Record

Policy

Medical records are secure, current, authenticated, legible, and complete.

Procedure

1. Entries in medical records are made only by individuals authorized to do so as specified in organization and medical staff policies.

2. All medical record entries are legible, complete, authenticated, timed and dated by the person responsible for making the entry. Prepared transcriptions of dictated reports, evaluations, and consultations must be reviewed by the author before authentication.

3. The authentication may include written signatures, first name, last name, and credential; computer key; signature key; or other methods approved by the governing body and medical staff to identify the name and discipline of the person making the entry.

4. Use of computer key or other methods to identify the author of medical record entry is not assignable or to be delegated to another person.

5. To avoid misinterpretation, symbols and abbreviations are used in the medical record only when they have been approved and there is an explanatory legend available to those authorized to make entries in the medical record and to those who must interpret them.

    5.1 Each abbreviation or symbol has only one meaning.

    5.2 A list of do-not-use abbreviations is also maintained.

6. All significant clinical information pertaining to a patient is entered into the medical record as soon as possible after its occurrence.

7. Medical records of discharged patients are submitted to Medical Records Department within fifteen days of discharge.

    7.1 A standardized filing order for the permanent record is used throughout the hospital and is available in Medical Records Department.

8. The records of discharged patients are completed within a period of time that does not exceed thirty days following discharge.

9. A medical record is considered complete when the required contents, including the discharge summary are assembled and authenticated, and when all final diagnoses and any complications are recorded, without use of symbols or abbreviations.

Implemented: 6-28-88
Revised: 5-23-89
Reviewed: 11-29-90

Revised: 6-92
Reviewed: 2-93
Revised: 11-94
Revised: 12-98
Revised: 3-02
Reviewed: 12-04
Revised: 6-06
Reviewed: 7-07
Reviewed: 5-09
Revised: 2-11
Revised: 9-13

Chapter: Medical Records (MR)
Section 4: Cosigning Documentation

Policy

Each discipline will develop guidelines that will assure professional and legal documentation standards are followed.

Procedure

1. Psychology

    1.1 All charting psychological reports and group notes completed by a psychology intern must be cosigned by a licensed psychologist.

2. Recreational Therapy

    2.1 All recreation therapy assessments completed by a therapeutic recreation technician must be cosigned by an MTRS (Master therapeutic Recreation Specialist or a TRS (Therapeutic Recreation Specialist).

    2.2 All progress notes and recreation assessments completed by a recreational therapy intern must be cosigned by a MTRS (Master Therapeutic Recreation Specialist) or a TRS (Therapeutic Recreation Specialist).

3. Occupational Therapy

    3.1 All progress notes and other documentation completed by psychiatric technicians in the occupational therapy department will be cosigned by an occupational therapist.

    3.2 All progress notes and occupational therapy assessments completed by occupational therapy students will be cosigned by an occupational therapist.

4. Social Work

    4.1 All documentation completed by a BSW (Bachelor of Social Work) intern must be cosigned by the USH staff who is their supervisor - either a CSW (Clinical Social Worker) or LCSW (Licensed Clinical Social Worker)

    4.2 All documentation completed by a first year MSW (Master of Social Work) intern must be cosigned by the USH staff who is their supervisor - either a CSW (Certified Social Worker) or LCSW (Licensed Clinical Social Worker).

    4.3 All documentation completed by a second year MSW intern must be cosigned by the USH staff who is their supervisor, an LCSW.

    4.4 Documentation completed by a USH staff who is a CSW or LCSWT (Licensed Clinical Social Worker Temporary) will be periodically reviewed and cosigned by their clinical supervisor (who is a LCSW) as per Utah Administrative Code R156-60a-601 (1)-(10).

Implemented: 7-20-99
Revised: 3-02
Reviewed: 12-04
Reviewed: 7-07
Revised: 5-09
Revised: 2-11
Reviewed: 9-13

Chapter: Medical Records (MR)
Section 5: Guidelines for Students and Interns

Policy

Undergraduate and graduate students who have clinical rotations at Utah State Hospital (USH) are supervised by a faculty member from their school. The director of the discipline corresponding to the student's area of practice is responsible for informing the university/college faculty member and the students of USH confidentiality policies and procedures.

Procedure

1. Student access to records is as follows:

    1.1. Students are limited to the records of patients with whom they are working.

    1.2 Unit treatment team designates patients appropriate for students.

    1.3 Students obtain access to USH electronic system by filling out an access request form per Technology Services policy.

    1.4 Students must sign an electronic record confidentiality agreement.

        1.4.1 The signed confidentiality agreement is maintained in the USH Education Department.

    1.5 The patients' right to have their records exempt from intern/student access will be honored upon the patients' request.

2. Student charting in the progress notes is as follows:

    2.1 Students chart in the progress notes with approval from the discipline director and supervision by appropriate staff member.

    2.2 All student entries are co-signed by the appropriate staff member.

    2.3 The discipline director orients students to USH charting guidelines.

    2.4 The following titles/abbreviations are used as part of the legal signature:

Nursing Discipline	**Abbreviation**
Student Nurse	SN
Occupational Therapy Discipline	**Abbreviation**
Occupational Therapy Student	OTS

Pharmacy Discipline	**Abbreviation**
Pharmacy Therapy Student	PhS
Medical Staff	**Abbreviation**
Medical Student	MdS
Psychology Discipline	**Abbreviation**
Psychology Intern	Psychology Intern
Physical Therapy Discipline	**Abbreviation**
Physical Therapy Intern	PTI
Recreational Therapy Discipline	**Abbreviation**
Student Recreational Therapist Intern	SRTI
Social Work Discipline	**Abbreviation**
Social Work Intern	SWI
Master Social Work Intern	MSWI

3. Student researchers must contact the Department of Human Services Institutional Review Board (IRB).

Implemented: 8-87
Revised: 6-88
Reviewed: 12-90
Revised: 7-92
Reviewed: 2-93
Revised: 11-94
Reviewed: 7-98
Revised: 3-02
Revised: 12-04
Reviewed: 7-07
Reviewed: 5-09
Revised: 2-11
Revised: 9-13

Chapter: Medical Records (MR)
Section 6: Forms Control

Policy

The Utah State Hospital Information Management/Medical Records Committee approves all chart forms. The USH Records Manager is the hospital forms controller. All chart forms are identified by a form number. Forms may not be implemented without proper approval.

Procedure

1. Employees request a new or change of a chart form through discipline director to the hospital Forms Controller.

2. The Forms Controller submits a draft form to applicable committees for input.

3. The draft form is then submitted to the Information Management/Medical Records Committee following input from applicable committees.

4. The Information Management/Medical Records Committee may recommend use of the form or may recommend a trial period.

    4.1. When a trial period is recommended, the form is used in a service area for a designated period of time to determine its need and usefulness.

    4.2. Following the trial period, a report is made to the Medical Records Committee.

    4.3. The Information Management/Medical Records Committee may then approve or deny use of the form.

5. Guidelines for using the form and, if applicable, distribution of NCR copies are included on the form.

6. Chart forms are designed to fit into a top-opening, five ring binder with a top margin of 1 inch.

7. Forms are printed with black ink.

8. Form identification is located on the bottom left side and patient identification is located on the bottom right side of the form.

9. Two-sided forms are printed in a head-to-foot style for tumble assembly in a chart.

10. Forms are normally printed on 8 1/2 inch by 11 inch paper.

Initiated: 2-94
Revised: 11-94
Reviewed: 7-98
Revised: 3-02
Revised: 12-04
Reviewed: 7-07
Revised: 5-09

Reviewed: 2-11
Reviewed: 9-13

Chapter: Medical Records (MR)
Section 7: Destruction of Documents Containing Confidential Patient Information

Policy

When documents containing patient information have met retention requirement and/or no longer have administrative value, they are destroyed by means of a high-security crosscut shredder.

Procedure

1. Documents to be shredded are collected in designated areas/shred bins in each service area.

2. Contracted document shredding company gathers documents to be shredded on a bi-weekly basis.

3. Shredding is completed by a contracted document shredding company.

4. Magnetic media, i.e., computer disks, floppy disks, video tape, etc. are sent to/collected by the Medical Records Department for proper disposal.

Implemented: 11-29-90
Revised: 4-92
Reviewed: 2-93
Revised: 11-94
Reviewed: 7-98
Revised: 3-02
Revised: 1-05
Reviewed: 7-07
Revised: 5-09
Reviewed: 2-11
Reviewed: 9-13

Chapter: Medical Records (MR)
Section 8: HIPAA Use and Disclosure of Protected Health Information

Purpose

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

Policy

1. Using and disclosing information for treatment, payment, and health care operations. (CFR 45 164.506)

    1.1. USH may use or disclose protected health information for treatment, payment, and health care operations (TPO) without the prior authorization of the individual. USH will agree to an individuals to request disclosure of PHI to a health plan if disclosure is for payment or operations, is not required by law, and the PHI pertains to services for which the individual has paid in full. (CFR 45 164.522)

        1.1.1. All requests for disclosure of protected health information are directed to the Medical Records Department. All requests for information are screened for approval by medical records personnel.

Procedure

1. USH may disclose protected health information without authorization for its own treatment activities or for the health care activities of another health care provider.

    1.1. Treatment means the provision, coordination, or management of "healthcare" and related services by one or more healthcare providers, including:

        1.1.1. The coordination or management of healthcare by a healthcare provider with a third party;

        1.1.2. Consultation between healthcare providers relating to a individual; or

        1.1.3. The referral of an individual for healthcare from one health care provider to another.

Examples: USH may contact a covered entity or healthcare provider to discuss the care of an individual who will soon be released form the hospital back to the community for outpatient treatment. The hospital and the local mental health center may exchange protected health information without prior authorization in order to plan the discharge and subsequent treatment of the individual. A physician may send without prior authorization a copy of an individual's medical record to healthcare providers who need the information to

treat the individual. In the event that a patient is transferred to another hospital/facility in on a medical separation transfer, the following information accompanies the patient: advance directives, if any, face sheet, medication administration record (MAR), current page of physician's orders, history and physical, pertinent medical progress notes, list of current medication, continuity of nursing care sheet, pertinent lab test/results, consultations, immunization record, and nursing emergency transfer sheet.

2. USH may disclose protected health information without authorization for its own payment activities or to another covered entity for that entity's payment activities.

    2.1. Payment means the activities undertaken to obtain or provide reimbursement for the delivery of health care includes:

        2.1.1. Eligibility or coverage determinations;

        2.1.2. Billings, collection activities, claims management, and related health care data processing;

        2.1.3. Medical necessity reviews, appropriateness of care, or justification of charges;

        2.1.4. Utilization reviews; and

        2.1.5. Disclosures to consumer reporting agencies related to collection of reimbursement.

Example: The State Hospital may disclose protected health information without prior authorization to an individual's health insurance company to determine eligibility and to seek reimbursement.
A caseworker believes an individual may be eligible for Medicaid benefits. The case manager may contact Medicaid to find out if the individual is enrolled and to initiate the claims process.

3. USH may use or disclose protected health information without authorization for its own healthcare operations.

    3.1. USH may disclose information without authorization to another covered entity for the health care operations of that entity, if:

        3.1.1. Both that entity and USH has or had a relationship with the individual who is the subject of the information;

        3.1.2. The information pertains to such relationship; and

        3.1.3. The disclosure is for the purpose of:

            3.1.3.1. Conducting quality assessment and improvement activities, including: outcome evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or

            3.1.3.2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice

or improve of their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; or

3.1.3.3. Detecting health care fraud and abuse or for compliance purposes.

Policy

2. Authorization for use and disclosure of protected health information. (45 CFR 164.508)

2.1. Except as otherwise permitted or required by law or these policies, USH shall obtain a completed and signed authorization for release of protected health information from the individual, or the individual's personal representative.

2.1.1. Following authorized disclosure of patient information, the signed authorization is retained in the patient record with notation of the specific information disclosed, the date of the disclosure, and the signature of the individual disclosing the information. Following authorized disclosure of patient information from a microfilmed or imaged record, the signed authorization is retained in the "Completed Releases on Microfilm or Imaged Records" file, with notification of the specific information disclosed, the date of the disclosure, and the signature of the individual disclosing the information.

Procedure

1. When an authorization is required.

1.1. A valid authorization is required in the following situations:

1.1.1. For disclosures to an employer for use in employment-related determinations;

1.1.2. For research purposes unrelated to the individual's treatment;

1.1.3. For any purpose in which federal law requires a signed authorization;

1.1.4. For disclosures to any person(s) designated by the individual; and

1.1.5. For use and disclosure of psychotherapy notes.

1.2. USH may obtain, use, or disclose information only if the written authorization includes all the required elements of a valid authorization. USH staff will use the approved "Authorization to Release Protected Health Information" form. A valid authorization must contain the following information:

1.2.1. A description of the information to be used or disclosed, that identifies the purpose of the information in a specific and meaningful fashion, except that "at the request of the individual" is sufficient when the individual initiates the authorization;

1.2.2. The name or other specific identification about the person(s) or class of person(s), authorized to make the specific use or disclosure;

1.2.3. The name or other specific identification of the person(s) or class of persons, to whom USH may make the requested use or disclosure;

1.2.4. An expiration date, or an expiration event that relates to the individual or to the purpose of the use or disclosure, and the expiration date/event has not yet expired;

1.2.5. Signature of the client, or of the client's personal representative, and the date of signature; and

1.2.6. If the individual's personal representative signs the authorization form instead of the individual, a description or explanation of the representative's authority to act for the individual, including a copy of the legal court document (if any) appointing the personal representative, must also be provided.

1.2.7. A description of the individual's right to revoke the authorization;

1.2.8. A description of how the protected health information may be re-disclosed and no longer have privacy protection.

1.3. Uses and disclosures must be consistent with and limited to what the individual has authorized on a signed authorization form.

1.4. An authorization must be voluntary and informed. USH may not require the individual to sign an authorization as a condition of providing treatment services, payment for health care services, except:

1.4.1. Before providing research-related treatment, USH may require the individual to sign an authorization for the use or disclosure of protected health information for such research; or

1.4.2. USH may require a individual to sign an authorization before providing health care that is solely for the purpose of creating protected health information for disclosure to a third party.

Example: An individual is applying for life insurance and the application requires the results of a physical exam be sent to a life insurance company. The health care provider conducting the exam may require the individual to authorize the release of the exam results to the life insurance company.

1.5. An authorization for use and disclosure of protected health information may not be combined with any other document to create a compound authorization, except for consents for research studies.

1.6. USH must provide a signed copy to the individual or the individual's personal representative when USH initiates the authorization.

1.7. USH must document and retain each signed authorization form for a minimum of six years from when it was revoked or expired.

Policy

3. Uses and disclosures not requiring authorization. (CFR 164.512)

3.1. To the extent required or permitted by law and these policies, USH may use or disclose protected health information without the written authorization of the client.

Procedure

1. When an authorization is not required:

   1.1. USH may disclose information without authorization to individuals who have requested disclosure of their information to themselves.

   1.2. Psychotherapy Notes: USH may use or disclose psychotherapy notes without written authorization of the individual only for:

      1.2.1. Use by the originator of the psychotherapy notes, for treatment purposes;

      1.2.2. Use or disclosures by USH in training programs where students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;

      1.2.3. When being used or disclosed by a health oversight agency in connection with oversight of the originator of the psychotherapy notes; or

      1.2.4. To the extent authorized under state law to defend USH in a legal action or other proceeding brought by the individual.

   1.3. Child Abuse Reporting: USH will use or disclose protected health information without written authorization of the individual if USH has reason to believe that a child is a victim of abuse or neglect. USH may disclose information to the Division of Child and Family Services or the nearest law enforcement agency.

   1.4. Adult Abuse Reporting: USH shall use or disclose information without written authorization of the individual if USH has reason to believe that an adult is a victim of abuse or neglect (elder abuse, nursing home abuse, or abuse of the mentally ill or developmentally disabled). USH may disclose protected information to Adult Protective Services or the nearest law enforcement agency:

      1.4.1. If the individual agrees to the disclosure, either orally or in writing; or

      1.4.2. When required by law (62A-3-304); or

      1.4.3. When USH staff, in the exercise of professional judgment believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

      1.4.4. When the individual is unable to agree because of incapacity, a law enforcement agency or other public official authorized to receive the report represents that:

         1.4.4.1. The protected information being sought is not intended to be used against the individual, and

         1.4.4.2. An immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

      1.4.5. When USH staff make a disclosure permitted above, USH must promptly inform the individual that such a report has been or will be made, except if:

         1.4.5.1. USH staff, in the exercise of professional judgment believes informing the individual would place the individual at risk of serious harm; or

1.4.5.2. USH staff would be informing a personal representative and USH staff reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the individual, as determined by USH staff, in the exercise of professional judgment.

1.5. Public Health: In accordance with Utah Law USH will disclose protected health information to a public health authority to prevent or control a disease, injury or disability.

1.6. Health Oversight: USH will disclose protected health information to a health oversight agency for oversight activities that are authorized by state and federal laws.

1.6.1 Types of oversight activities include:

1.6.1.1. Audits;

1.6.1.2. Civil, administrative, or criminal investigations;

1.6.1.3. Inspections;

1.6.1.4. Licensure or disciplinary actions;

1.6.1.5. Civil, administrative, or criminal proceedings or actions; or

1.6.1.6. Other activities necessary for oversight of the health care system, government benefit programs, determining compliance with program standards.

1.6.1.7. If a health oversight activity is conducted in conjunction with an oversight activity involving a non-health claim for public benefits, the joint activity is considered a health oversight activity and the disclosure may be made.

Exception: A health oversight activity does not include:

1.6.2. The individual is the subject of the investigation or activity; and

1.6.3. The investigation or activity does not relate to the following:

1.6.3.1. Receipt of health care;

1.6.3.2. Claim for public benefits related to health, or qualification for, or receipts of public benefits or services when an individual's health is integral to the claim for the benefits or services.

1.7. Judicial and Administrative Proceedings: USH may disclose protected health information in response to an order of a court or administrative tribunal, provided that USH discloses only the protected health information authorized by the order.

1.7.1. USH may disclose protected health information in response to a subpoena, discovery request, or other lawful process, without a court order if one of the following circumstances applies:

1.7.1.1. USH receives satisfactory assurance from the party seeking the protected health information that reasonable efforts have been made to ensure that the individual who is the subject of the protected health information has been given notice of the request for the protected health information by providing USH with a written statement and documentation demonstrating that:

1.7.1.1.1. A good faith effort was made to provide a written notice to the individual;

1.7.1.1.2. The notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal; and

1.7.1.1.3. The time for the individual to raise objections has elapsed, and;

1.7.1.1.4. No objections were filed, or

1.7.1.1.5. All objections filed by the individual have been resolved by the court or administrative tribunal and the disclosures being sought are consistent with such resolution.

1.7.1.2. USH receives satisfactory assurance from the party seeking the protected health information that reasonable efforts have been made by USH to secure a qualified protective order.

1.7.1.2.1. The party seeking protected health information must Provide USH with a written statement and documentation demonstrating that:

1.7.1.2.1.1. The parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or

1.7.1.2.1.2. The party seeking PHI has requested a qualified protective order from a court or administrative tribunal

1.7.1.2.2. A "qualified protective order" means an order of the court or administrative tribunal or stipulation by the parties that:

1.7.1.2.2.1. Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceed-ing for which the information was requested; and

1.7.1.2.2.2. Requires the return or destruction of the protected health information (including all copies) at the end of the litigation or proceeding.

1.7.2 USH may disclose protected health information without receiving satisfactory assurances from the party seeking the information if the USH makes reasonable efforts to provide notice to the individual, meeting the requirement of 1.7.1.1 above, or seeks a qualified protective order meeting the requirements of 1.7.1.2 above.

1.8. Law Enforcement: USH may use or disclose protected health information to law enforcement officials without the written authorization of the individual for the following law enforcement purposes.

1.8.1. USH shall disclose protected health information, in accordance with UCA 26-23a-2, to report wounds or other physical injuries caused by the use of a deadly weapon (knife, gun, or explosive device).

1.8.2 USH may disclose information in compliance with, and limited to the relevant specific requirements of:

1.8.2.1 A court order or warrant, summons, or subpoena issued by a judicial officer;

1.8.2.2. A grand jury subpoena; or

1.8.2.3. An administrative request, including administrative subpoena or summons, a civil or authorized investigative demand, or similar lawful process, provided that the information is relevant, material, and limited to a legitimate law enforcement inquiry, and de-identified information could not reasonably be used.

1.8.3. USH may disclose limited protected health information upon request of a law enforcement official without authorization for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

1.8.3.1. The information USH may disclose is limited to:

1.8.3.1.1. Name and address;

1.8.3.1.2. Date and place of birth;

1.8.3.1.3. Social security number;

1.8.3.1.4. ABO blood type or RH factor;

1.8.3.1.5. Type of injury;

1.8.3.1.6. Date and time of treatment;

1.8.3.1.7. Date and time of death if applicable; and

1.8.3.1.8. A description of distinguishing physical characteristics including height, weight, gender, race, hair, and eye color, presence or absence of beard or mustache, scars, and tattoos. In cases of criminal court commitments, a photo-graph may be provided.

Exception: USH may not disclose, for purposes of identification or location, protected health information related to the subject's DNA or DNA analysis, dental records, or typing, samples, or analysis of bodily fluids or tissues.

1.9 Crime Victims: USH may disclose protected health information upon request to a law enforcement official about an individual who is or is suspected to be the victim of a crime, if:

1.9.1. USH is otherwise authorized by law to disclose that information for purposes of an abuse reporting law or for public health or health oversight purposes; or

1.9.2. The individual agrees to the disclosure, either orally or in writing; or

1.9.3. USH is unable to obtain the individual's agreement due to incapacity or emergency circumstance, if:

1.9.3.1. The law enforcement official represents that such information is needed to determine whether a violation of law by someone other than the victim has occurred and such information is not intended for use against the victim;

1.9.3.2. The law enforcement official represents that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

1.9.3.3. USH determines that the disclosure is in the best interests of the individual.

1.9.4. USH may disclose protected health information to a law enforcement official about an individual who has died, for the purpose of alerting law enforcement of the death, if USH suspects that death may have resulted from criminal conduct.

1.9.5. USH may disclose protected health information to a law enforcement official if USH believes in good faith that the information constitutes evidence of criminal conduct on USH premises.

1.9.6. USH may use or disclose protected health information, if consistent with applicable law and standards of ethical conduct, when in good faith it believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the use or disclosures is to person(s) reasonably able to prevent or lessen the threat, including the target of the threat, or except that the use or disclosure may not be made if the statement is made in the course of treatment for the criminal conduct that is the basis of the statement, counseling, therapy or in the course of requesting treatment, counseling, or therapy;

1.9.6.1. Who has made a statement admitting participation in a violent crime that USH reasonably believes may have caused serious harm to the victim, or for law enforcement authorities to identify or apprehend an individual.

1.9.6.2. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

1.10. Government Functions: USH may disclose protected health information without the authorization of the individual for the following specialized government functions unless federal or state law prohibits such disclosure.

1.10.1. For individuals who are Armed Forces personnel, as deemed necessary by appropriate military command authorities to ensure the proper execution of the military mission, when an appropriate notice is published in the Federal Register

1.10.2. To authorized federal officials for conducting lawful intelligence, counter-intelligence, and other national security activities, as authorized by the federal National Security Act (50 U.S.C. 401, et seq.) and implementing authority.

1.10.3. To authorized federal officials for the protection of the President or of other persons authorized by applicable federal law.

1.10.4. To the United States Department of Health and Human Services when required to investigate or determine USH compliance with HIPAA.

1.11. Correctional Institutions: USH may disclose protected health information without the written authorization of the individual to a correctional institution or a law enforcement official having lawful custody of that individual, if the institution or official represents that the information is necessary for:

1.11.1. Providing health care to the person;

1.11.2. The health or safety of the individual or of other inmates;

1.11.3. The health and safety of the officers, employees, or others at the correctional institution;

1.11.4. The health and safety of the individual and officers or other person responsible for transporting inmates;

1.11.5. The administration and maintenance of the safety, security, and good order of the correctional institution. The State Hospital Forensic Unit may use protected health information of inmates for any purpose for which protected health information could be disclosed.

1.12. Workers Compensation: USH may disclose protected health information to the extent necessary to comply with workers' compensation laws or laws relating to other similar programs that are established by law and provide benefits for work-related injuries or illness.

1.13. Disaster Relief: USH may use or disclose protected health information to federal, state, or local government agencies engaged in disaster relief activities, as well as private disaster assistance organization (Red Cross) for the purpose of coordinating the notification of a family member, personal representative, or other person responsible for the individual's care, of the individual's location, general condition or death.

1.14. Organ/Tissue Donation: USH will disclose protected health information, in accordance with UCA 26-28-6, to an appropriate procurement organization for the purpose of facilitating organ, tissue, eye, or other body part donation and transplantation.

1.15. Coroners, Medical Examiners, and Funeral Directors: USH may disclose protected health information without authorization for the purpose of identifying a deceased person, determining a cause of death, or duties authorized by law, to coroners and medical examiners. USH may disclose protected health information to funeral directors, consistent with Utah law, as required to carry out their duties.

Policy

4. Client authorization is not required if informed in advance and given a chance to object.

4.1. USH may use or disclose protected health information for a facility directory and for involving family members or friends in the individual's care, provided that the individual is informed in advance and has been given the opportunity to either agree, to refuse, or restrict the use or disclosure.

Procedure

1. Use and disclosure for facility directories:

1.1. Except when the individual objects, USH may:

1.1.1. Use the following protected health information to maintain a directory of individuals in its facility:

1.1.1.1. Name

1.1.1.2. Location in the facility; and

1.1.1.3. Religious affiliation

1.1.2. Disclose for directory purposes:

1.1.2.1. To members of the clergy, the individual's name, location and religious affiliation;

1.1.2.2. To all other persons who ask for the individual by name, the individual's location in the facility.

1.2. Before using the protected health information for a facility directory, USH must:

1.2.1. Inform the individual of the protected health information that may be included in the directory and the person to whom it may be disclosed; and

1.2.2. Provide the individual the opportunity to restrict or prohibit some or all of the uses or disclosures.

1.2.2.1. The individual will complete the "Patient Objection to being listed in Patient Directory" form to indicate if they wish to restrict some or all of the information listed in the patient directory.

1.2.2.2. If it is not practicable to provide an opportunity to object because of the individual's incapacity or an emergency treatment circumstance, USH may use or disclose some or all of the protected health information for the facility's directory, if the disclosure is:

1.2.2.2.1. Consistent with the individual's prior expressed preference, if any, that is known to USH; and

1.2.2.2.2. In the individual's best interest as determined by USH, in the exercise of professional judgment.

1.2.2.2.3. USH must inform the individual and provide an opportunity to object to uses or disclosures when it becomes practicable to do so.

2. Use and Disclosure for notifying family or friends:

2.1. USH may use and disclose protected health information to a family member, other relative, or close personal friend of the individual, or any other person named by the individual, subject to the following limitations:

2.1.1. USH may reveal only the protected information that directly relates to such person's involvement with the individual's care or payment for such care.

2.1.2. USH may use or disclose protected information for notifying (including identifying or locating) a family member, personal representative, or other person responsible for care of the individual, regarding the individual's location, general condition, or death.

2.1.3. If the individual is present for, or available prior to, such a use or disclosure and has the capacity to make healthcare decisions, USH may disclose the protected information if it:

2.1.3.1. Obtains the individual's agreement to disclose to the third parties involved in his/her care;

2.1.3.2. Provides the individual an opportunity to object to the disclosure, and the individual does not express an objection; or

2.1.3.3. Reasonably infers from the circumstances that the individual does not object to the disclosure.

2.1.4. If the individual is not present, or the opportunity to object to the use or disclosure cannot practicable be provided due to the individual's incapacity or an emergency situation, USH may determine, using professional judgment, whether the use or disclosure is in the individual's best interests and if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

2.1.4.1. Any agreement, objection, refusal, or restriction by the individual, may be oral or in writing. USH will document any such oral communication in the client's case file.

2.1.4.2. USH will also document in the case file the outcome of any opportunity provided to object; the individual's decision not to object; or the inability of the individual to object.

Exception: Oral permission to use or disclose information for purposes described subsection (a) of this section is not sufficient when the individual is referred to or receiving alcohol and drug abuse treatment. Written authorization is required under these circumstances.

Policy

5. Re-disclosure of an individual's information:

5.1. Unless prohibited by state and federal laws, information held by USH and authorized by the individual for disclosure may be subject to re-disclosure and no longer protected by USH policy. Whether or not the information remains protected depends on whether the recipient is subject to federal laws, court protective orders or other lawful process.

5.2. Federal regulations (42 CFR part 2) prohibit USH from making further disclosure of alcohol and drug treatment information without the specific written authorization of the individual to whom it pertains.

Policy

6. Revocation of an authorization

6.1. A client may revoke in writing an authorization at any time.

Procedure

1. An individual must complete the Revocation of Authorization section, to revoke a written authorization to disclose information. USH must boldly mark the original authorization form "revoked."

2. When an individual revokes only one record holder on the authorization form, USH will boldly mark that section only "revoked" and include the date and the individual's signature.

3. Revoked authorization forms must be maintained in the individual's file.

4. No revocation applies to information already released while the authorization was valid and in effect.

Policy

7. Verification of individuals requesting information. (45 CFR 164.514)

7.1. Protected health information may not be disclosed without verifying the identity of the person requesting the information and the authority of such person to have access to protected health information if the person and their authority is not known to the USH staff member fulfilling the request.

Procedure

1. USH may rely on any of the following to verify identity of a public official or a person acting on behalf of the public official:

1.1. Agency identification badge, or other proof of government status;

1.2. A written statement on appropriate governmental letterhead;

1.3. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority, or other evidence such as a contract for services, memorandum of understanding, or purchase order.

2. For all other requesters, any of the following may be relied upon to verify identity:

2.1. Identification badge;

2.2. Driver's license or other government issued identification;

2.3. Written statement of identification on agency letterhead; or

2.4. Similar proof

3. Verification of Authority

3.1. Legal documentation that includes the authority to make health care decisions on behalf of the individual.

Policy

8. Denial of requests for information

8.1. Unless an individual has signed an authorization, or the information about the individual can be disclosed pursuant to this policy, USH denies any request for protected health information.

9. Records containing identifying information other than that of the patient or staff may be redacted.

10. Documents containing patient information may be transmitted by FAX (facsimile machine) with the expectation that the following have occurred:

10.1. Verification that receiving FAX machine is located in a secure area,

10.2. Verification of receiving FAX number, and

10.3. A cover sheet stating that the transmittal contains confidential and privileged information intended for the use of the recipient, prohibiting any dissemination or copying by unauthorized individuals, and giving instructions for transmittals received in error is sent with all patient information being faxed.

11. Fees for copies of records are defined in Department of Human Services Rule (R495-810-2).

Implemented: 6-03
Revised: 1-05
Reviewed: 7-07
Revised: 10-10
Revised: 9-13

Chapter: Medical Records (MR)
Section 9: HIPAA Administrative, Technical, and Physical Safeguards

Policy

USH acquires, creates, accesses, uses, discloses, transmit, maintains, and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

USH establishes appropriate administrative, technical, and physical safeguards to protect the Privacy of protected health information.

Procedure

1. General

    1.1. USH must take reasonable steps to safeguard protected health information from any intentional or unintentional access, acquisition, use or disclosure of PHI that is in violation of HIPAA and the USH privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral, and visual representations of confidential information. (45 CFR 164.530)

2. Safeguarding protected health information - USH workplace practices.

    2.1. Paper:

        2.1.1 Each USH workplace stores records containing protected health information in locked rooms or storage systems.

        2.1.2 USH staff must make reasonable efforts to ensure the safeguarding of protected health information.

        2.1.3 Each USH workplace ensures that records awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.

        2.1.4 Each USH workplace ensures that shredding of records is performed on a timely basis, consistent with record retention requirements.

        2.1.5 Patient records are not removed from the premises except when required for treatment, payment, healthcare operations or when authorized by law.

        2.1.6 All records no longer in active use must be sent to the Medical Records Department for proper management, storage, retention and destruction.

2.1.7 No protected health information is used, maintained or stored by treating units or practitioners after 45 days post discharge of patient.

2.2. Electronic

2.2.1 Staff is responsible for all entries and queries performed under their unique computer identity.

2.2.2 Individuals obtain system access and log in as specified in Technology Services policy and procedure.

2.2.2.1 Remote access may be granted to individuals who have a verified business necessity.

2.2.2.1.1 Individuals approved for remote access must complete a Remote Access Request Form which is reviewed and approved by USH Executive Staff.

2.2.2.1.2. Signed form is maintained by the Privacy Officer.

2.2.2.2. All USH mobile devices must have and use encryption software.

2.2.3. Personal Identification Numbers (PIN) for electronic signatures are used.

2.2.3.1. PIN is not used by any other individual.

2.2.4. Computer workstations have a screen saver password in place.

2.2.4.1. Staff do not leave their computer workstation without initiating system lockout or signing off.

2.2.4.1.1. E-Chart has an automatic lockout when no activity is detected for 10 minutes.

2.2.5. Protected health information is only saved on network (h) or controlled access (f) drives.

2.2.5.1. Privacy Officer conducts random audits of employee computer drives.

2.2.6. If any protected health information is necessary to be included in email communication, the sender must use encrypted, secure email process.

2.2.6.1. Only patient initials are used as identification in email correspondence.

2.2.6.2. No protected health information is used, maintained or stored by treating units or practitioners after 45 days post discharge of patient.

2.2.7. Audits of access to electronic records are conducted at least bi-annually in addition random audits based upon unique circumstances, i.e., high profile patients, staffing concerns, etc.

2.2.7.1. When questionable access is detected a request for explanation is sent to the employee and their supervisor for follow-up.

2.2.7.2. If it is determined that the access was inappropriate the supervisor follows up with appropriate sanctions following DHRM and DHS rules.

2.2.7.3. Follow-up by supervisor is reported to the Privacy Officer.

2.2.8. Electronic recording

2.2.8.1. Workforce

2.2.8.1.1. Electronic recording devices, audio or video, such as cameras, camera phones, minicams, tape recorders, palm pilots, PDA's (personal digital assistants), etc., are not used by any person for the recording of patients without prior, written HIPAA Compliant authorization using USH approved form USH-205-1010. Exception: Authorization would not be required for USH surveillance camera's.

2.2.8.1.2. A patient may give informed consent for videotaping, photographing or recording by completing an authorization form (USH-205-1010.

2.2.8.1.2,1 USH Security Officers may take digital photos of a patient when there has been an injury.

2.2.8.1.3. All recordings which are not specifically authorized to be disclosed outside of USH must be sent to the Medical Records Department for proper management, storage, retention and destruction.

2.2.8.1.4. No protected health information is used, maintained or stored by treating units or practitioners after 45 days post discharge of patient.

2.2.8.2. Media

2.2.8.2.1. When a request for interview/recording by media is received the Public Information Officer for the Department of Human Services is notified.

2.2.8.2.2. Patient authorization must be obtained by completing USH media authorization form (USH-205-1010) prior to any disclosure.

2.2.9. Electronic storage devices containing protected health information are not taken off hospital grounds.

2.2.9.1. Electronic storage devices that contain, or ever have contained, protected health information must be sent to the Medical Records Department for proper management, storage, retention and destruction.

2.2.9.2. No protected health information is saved to any type of removable media, i.e., jump drives, disk, etc.

2.2.9.3 No protected health information is used, maintained or stored by treating units or practitioners after 45 days post discharge of patient.

2.2.10. USH limits use of smart phones and other mobile data devices that create, store, access, transmit or receive e-mails via the State of Utah system whether hospital issued or personal. Smart phones and other mobile data devices that are used to create, store, access, transmit or receive e-mails via the State of Utah system must meet the following criteria:

a. Install Mobile Device Management software on their device prior to connecting them to State systems.

b. The user must use a password to access the mobile device and have encryption software enabled.

c. Software must be kept up to date. The user must use the most recent operating system available for their mobile data device and the user must apply security updates for any other software in a regular and timely manner unless instructed otherwise by the hospital.

2.2.11. USH prohibits staff from posting any patient related protected health information, even if the patient is not identified, on social media sites whether at work or on personal time.

2.2.11.1. USH employees are not allowed to discuss patient-related information on blogs, social media, and other Internet platforms.

2.2.11.2. Posting stories or pictures about nameless patients is also prohibited (it is a HIPAA violation).

2.2.11.3. It is every hospital employee's obligation to notify their supervisor and the privacy officer (Tonya Smith in Medical Records ext 44219) if they come across anything on social media sites that is a suspected breach of confidentiality.

2.2.11.4. An inventory of mobile data devices owned by the hospital is maintained in the Business Office.

2.3. Oral

2.3.1. USH staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of protected health information, regardless of where the discussion occurs.

2.3.1.1. Patient information may only be discussed with authorized individuals for authorized purposes.

2.3.1.1.1. Discussions are not held where other patients, staff, or visitors not directly involved in patient's care can be overheard.

3. Exception: In work environments structured with few offices or closed rooms, incidental uses or disclosures of protected health information may occur when discussions are overheard. Such

incidental uses or disclosures are not considered a violation provided that reasonable safeguards are utilized and USH complies with the minimum necessary requirement where applicable. (45 CFR 164.502)

3.1.1. Each USH workplace must foster workforce awareness of the potential for inadvertent verbal disclosure of protected health information.

3.2. Visual

3.2.1. USH must ensure that protected health information is adequately shielded from unauthorized disclosure on computer screens, information boards, and paper documents.

4. Safeguarding protected health information - USH administrative safeguards.

4.1. USH identifies the employees or classes of employees who need access to protected health information to carry out their duties.

4.1.1. For each person or class of persons, managers/supervisors identify the categories of protected health information to which access is needed, and identify any conditions appropriate to the access.

4.2. USH conducts periodic and random reviews of the effectiveness of the administrative safeguards.

4.3. All members of USH workforce are required to read and sign the “Access and Confidentiality Agreement” form

4.3.1. This form is filed in the individual's personnel file in the Human Resource Office.

5. Members of the USH workforce report all suspected intentional and/or accidental violations of security and privacy policies and procedures to the Privacy Officer.

Implemented: 6-03
Revised: 10-04
Revised: 1-05
Revised: 9-05
Reviewed: 7-07
Revised: 10-10
Revised: 8-12
Revised: 8-13

Chapter: Medical Records (MR)
Section 10: HIPAA Business Associate Relationships

Policy

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

USH discloses an individual's protected health information to a business associate of USH and specifies provisions that must be included in USH contracts with business associates.

Procedure

1. General

1.1. A business associate is a person or entity who:

1.1.1. On behalf of USH creates, receives, transmits protected health information.

1.1.1.1. A function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or

1.1.1.2. Any other function or activity regulated as part of the Administrative Simplification Provisions of HIPAA; or

1.1.2. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for USH, where the provision of the service involves the disclosure of individually identifiable protected health information to the person providing the service.

1.2. A business associate includes a subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate.

1.3. The following are not business associates or business associate relationships:

1.3.1. USH employees, volunteers, trainees, or others under the direct control of USH, whether or not they are paid by USH;

1.3.2. Medical providers providing treatment to individuals;

1.3.3. Enrollment or eligibility determinations, involving individuals served by USH, between government agencies;

1.3.4. Payment relationships, such as when USH is paying medical providers, or other entities for services to an individual, when providing services that are not on behalf of USH;

1.3.5. When an individual's protected health information is disclosed based solely on an individual's authorization; by USH or created for USH; and

1.3.6. When the only information being disclosed is information that is de-identified in accordance with De-identification of Protected Health Information and Use of Limited Data Sets policy.

1.4. USH may disclose an individual's protected health information to a business associate and may allow a business associate to create, receive, maintain or transmit an individual's protected health information on behalf of USH, if:

1.4.1. USH enters into a written contract, or other written agreement or arrangement, with the business associate before disclosing an individual's protected health information to the business associate;

1.4.2. The written contract or agreement provides satisfactory assurance that the business associate will safeguard the protected health information and comply with the applicable standards, implementation specifications and requirements of HIPAA, including but not limited to electronic PHI.

2. Business associate contract requirements

2.1. A contract between USH and a business associate must include terms and conditions that:

2.1.1. Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to access, acquire, use or disclose protected health information in a manner that would violate HIPAA or USH privacy policies, except that the contract may permit the business associate to:

2.1.1.1. Access, acquire, use and disclose protected health information for the proper management and administration of the business associate; and

2.1.1.2. Provide data segregation services related to USH healthcare operations.

2.1.2 Provide that the business associate will:

2.1.2.1. Not use or further disclose protected health information other than as permitted or required by the contract or as required by law;

2.1.2.2. Use safeguards to prevent use or disclosure of the protected health information that are not permitted by the contract;

2.1.2.3. Report to USH anytime it becomes aware of a use or disclosure of protected health information not permitted by HIPAA or the contract;

2.1.2.4. The business associate must notify USH within one business day of the discovery of a suspected intentional or accidental breach of unsecured protected health information.

2.1.2.4.1. To the extent possible, the business associate should provide the covered entity with identification of each individual reasonably believed to be affected by the breach as well as any information required to be provided by the covered entity in it's notification to affected individuals.

2.1.2.4.1.1. A brief description of what happened, including the date of the breach, the date of the discovery of the breach

2.1.2.4.1.2. A description of the types of protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

2.1.2.4.1.3. A brief description of what was done to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

2.1.2.5. Ensure that any agents or subcontractors to whom it provides protected health information agrees, through a business associate agreement, to the same restrictions and conditions that apply to the business associate;

2.1.2.6. Make protected health information available so that USH may comply with a request from an individual to inspect and copy protected health information, amend protected health information or obtain an accounting of disclosures as required by the Privacy Rights of Individuals policy.

2.1.2.7. Incorporate amendments to protected health information when notified to do so by USH;

2.1.2.8. Makes its internal practices, books, and records relating to the use and disclosure of protected health information available to USH and to the United States Department of Health and Human Services for the purpose of determining compliance with federal requirements; and

2.1.2.9. At termination of the contract, if feasible, return or destroy all protected health information that the business associate still maintains in any form. If return or destruction is not feasible, the business associate will continue to protect the information.

2.1.3. Authorize termination of the contract if USH determines that the business associate has violated a material term of the contract.

2.2. If the business associate of USH is another governmental entity:

2.2.1. USH may enter into a memorandum of understanding, rather than a contract, with the business associate if the memorandum of understanding contains terms that accomplish the same objectives as the business associate agreement; or

2.2.2. USH is not required to enter into a business associate agreement, if other laws or regulations contain requirements applicable to the business associate that accomplish the same objectives as the business associate agreement.

2.3. If a business associate is required by law to perform a function that qualifies it as a business associate, USH must make a good faith attempt to obtain satisfactory assurances but if it fails:

2.3.1. USH may disclose protected health information to the business associate to the extent necessary to comply with the legal requirements without obtaining satisfactory assurances; and

2.3.2. USH must document its good faith attempt and the reason for the failure.

2.4. The written contract or agreement between USH and the business associate may permit the business associate to:

2.4.1. Use information it receives in its capacity as a business associate to USH if necessary:

2.4.1.1. For proper management and administration of the business associate; or

2.4.1.2. To carry out legal responsibilities of the business associate.

2.4.2. Disclose information it receives in its capacity as a business associate for the purposes in subsection above, if:

2.4.2.1. The disclosure is required by law; or

2.4.2.2. The business associate receives reasonable assurances from the person to whom the protected health information is disclosed that:

2.4.2.2.1. It will be held confidentially and used or disclosed further only as required by law or for the purposes to which it was disclosed to such person; and

2.4.2.2.2. The person notifies the business associate of any known instances in which the confidentiality of the information has been breached.

3. Responsibilities of USH in Business Associate relationships

3.1. USH responsibilities in business associate relationships include, but are not limited to, the following:

3.1.1. Receiving and logging an individual's complaints regarding the uses and disclosures of protected health information by the business associate;

3.1.2. Receiving and logging reports from the business associate of possible violations of the business associate contracts;

3.1.3. Implementation of corrective action plans, as needed; and

3.1.4. Mitigation, if necessary, of known violations up to and including contract termination.

3.2. USH will provide business associates with applicable contract requirements and may provide consultation to business associates as needed on how to comply with contract requirements regarding protected health information.

4. Business associates non-compliance

4.1. If USH knows of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligation under the contract, USH must take reasonable steps to cure the breach or end the violation, as applicable, including working with and providing consultation to the business associate.

4.2. If such steps are unsuccessful, USH must:

4.2.1. Terminate the contract or arrangement, if feasible; or

4.2.2. If termination is not feasible, report the problem to the United States Department of Health and Human Services.

Implemented: 6-03
Reviewed: 1-05
Reviewed: 7-07
Reviewed: 5-09
Revised: 10-10
Revised: 8-13

Chapter: Medical Records (MR)
Section 11: HIPAA De-identification of Client Information and Use of Limited Data Sets

Policy

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

Protected health information is used and disclosed if the information that identifies an individual has been removed or restricted to a limited data set.

Procedure

1. Requirements for de-identification of protected health information

    1.1. De-identified information is protected health information which USH or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify an individual.

    1.2. Unless otherwise restricted or prohibited by other federal or state law, USH may use and disclose protected health information, without further restriction, if USH or another entity has taken steps to de-identify the information consistent with the requirements and restrictions of this policy.

    1.3. Protected health information is sufficiently de-identified, and cannot be used to identify an individual, only if:

        1.3.1. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

            1.3.1.1. Has applied these principles and methods, and determined that the risk is minimal that the information could be used, alone or in combination with other reasonably available information, by a recipient of the information to identify the person whose information is being used; and

            1.3.1.2. Has documented the methods and results of the analysis that justify such a determination; or

        1.3.2. The following identifiers of the individual or of relatives, employers, and household members of the individual are removed:

            1.3.2.1. Names;

1.3.2.2. All geographic subdivisions smaller than a State, including street address, city, county, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic units containing 20,000 or fewer people is changed to 000;

1.3.2.3. All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into single category of "age 90 or older;"

1.3.2.4. Telephone numbers;

1.3.2.5. Fax numbers;

1.3.2.6. Electronic mail addresses;

1.3.2.7. Social security numbers;

1.3.2.8. Medical record numbers;

1.3.2.9. Health plan beneficiary numbers;

1.3.2.10. Account numbers;

1.3.2.11. Financial identifiers;

1.3.2.12. Certificate or license numbers;

1.3.2.13. Vehicle identifiers and serial numbers, including license plate numbers;

1.3.2.14. Device identifiers and serial numbers;

1.3.2.15. Web Universal Resource Locators (URLs);

1.3.2.16. Internet Protocol (IP) address numbers;

1.3.2.17. Biometric identifiers, including fingerprints and voiceprints;

1.3.2.18. Full face photographic images and any comparable images; and

1.3.2.19. Any other unique identifying number, characteristic, or codes, except as permitted under subsection C, above, of this policy; and

1.3.3. USH has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

1.4. The USH Privacy Officer will designate the statistician or other person who may be either:

1.4.1. A USH employee;

1.4.2. An employee of another governmental agency; or

1.4.3. An outside contractor or consultant.

1.5. Protected health information which has been de-identified as described above is not individually identifiable and the USH privacy policies do not apply unless the information is re-identified.

2. Re-identification of de-identified information

2.1. USH may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by USH provided that:

2.1.1. The code or other means of record identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and

2.1.2. USH does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

2.1.3. Disclosure of a code or other means of record identification constitutes disclosure of protected health information. USH may use or disclose codes, other means of record identification, or re-identified information only after complying with all USH privacy policies.

3. Requirements for a limited data set

3.1. USH may use protected health information to create a limited data set or disclose protected health information to a business associate to create a limited data set.

3.2. USH may disclose a limited data set only for the purposes of research, public health, or health care operations.

3.3. A limited data set is protected health information that excludes the following direct identifiers of the individual, or of relatives, employers or household members of the individual:

3.3.1. Names;

3.3.2. Postal address information, other than town or city, State and zip code;

3.3.3. Telephone numbers;

3.3.4. Fax numbers;

3.3.5. Electronic mail addresses;

3.3.6. Social Security numbers;

3.3.7. Medical record numbers;

3.3.8. Health plan beneficiary numbers;

3.3.9. Account numbers;

3.3.10. Financial identifiers;

3.3.11. Certificate/license numbers;

3.3.12. Vehicle identifiers and serial numbers, including license plate numbers;

3.3.13. Device identifiers and serial numbers

3.3.14. Web Universal Resource Locator (URLs);

3.3.15. Internet Protocol (IP) address numbers;

3.3.16. Biometric identifiers, including finger and voice prints; and

3.3.17. Full face photographic images and any comparable images.

4. Data use agreement

4.1. USH may use or disclose a limited data set only if USH enters into a written data use agreement with the recipient of the limited data set.

4.2. A data use agreement must:

4.2.1. Specify the permitted uses and disclosures (research, public health, or health care operations only) of such information by the limited data set recipient. USH may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this policy if done by USH.

4.2.2. Specify who is permitted to use or receive the limited data set; and

4.2.3. Specify that the limited data set recipient will:

4.2.3.1. Not use or further disclose the information other than as specified in the data use agreement or as otherwise required by law;

4.2.3.2. Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the data use agreement;

4.2.3.3. Report to USH any use or disclosure of the information not specified in its data use agreement;

4.2.3.4. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

4.2.3.5. Not identify the information or contact the individuals whose data is being disclosed.

4.3. USH takes reasonable steps to cure any breach of the data use agreement or any violations by the limited data set recipient. If such steps are unsuccessful, USH will discontinue disclosure of protected health information to the limited data set recipient and report the problem to the United States Department of Health and Human Services.

Implemented: 6-03
Reviewed: 1-05
Reviewed: 7-07
Reviewed: 5-09
Revised: 10-10
Revised: 9-13

Chapter: Medical Records (MR)
Section 12: HIPAA Enforcement, Sanctions, and Penalties for Violations of Individual Privacy

Policy

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information (PHI) in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the HITECH Omnibus Rule.

USH safeguards protected health information and minimize the risk of unauthorized access, acquisition, use, or disclosure.

Procedure

1. General

1.1. All members of the USH workforce (employees, volunteers, interns, and others under the direct control of USH) and its business associates and their subcontractors must guard against improper access, acquisition, use or disclosures of protected health information.

1.1.1. Members of the USH workforce who are uncertain if an access, acquisition, use or disclosure of protected health information is permitted shall consult with their privacy officer prior to engaging in the access, acquisition, use or disclosure of protected health information.

1.2. All members of the workforce are required to be aware of their responsibilities under HIPAA and the USH privacy policies.

1.2.1. All members of the workforce are required to participate in training and then to sign the "Access & Confidentiality Agreement" form, indicating they understand and agree to abide by HIPAA and the USH privacy policies.

1.2.2. USH employees who violate HIPAA or the privacy policies are subject to corrective action or discipline consistent with the Utah State Department of Human Resource Management Rules, including but not limited to termination of employment.

1.2.3. Volunteers, interns, and others under the direct control of USH who violate HIPAA or the privacy policies are subject to having their association with the USH terminated.

1.3. Any member of the USH workforce, it's business associates and their subcontractors who violates HIPAA may be personally subject to criminal prosecution and monetary penalties.

1.4. Any use or disclosure of PHI in a manner not permitted under HIPAA is presumed to be a breach.

2. Definition of Breach

2.1. A breach is an unauthorized acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of PHI.

2.1.1. A breach is not an

2.1.1.1 Unintentional, good faith acquisition, access, or use of PHI within the scope of employment if the PHI is not further acquired, accessed, used or disclosed by any person; or an inadvertent disclosure of PHI from a person authorized to access PHI to another person authorized to access PHI at the same facility when the PHI is not further acquired, accessed, used or disclosed without authorization.

2.1.1.2 Inadvertent disclosure.

2.1.1.3 Good faith belief that unauthorized person would be reasonably have been able to retain the information.

3. Breach Investigation

3.1. Each breach and suspected breach shall be reported to the Privacy Officer as soon as it is discovered.

3.1.1. A breach of PHI shall be treated as “discovered” as of the first day of which such breach is known to the organization.

3.2. The Privacy Officer shall investigate each suspected breach.

3.2.1 The investigation shall include a review of the information that was potentially breached, interviews with the patients and staff involved, gathering any additional information and supporting documents to determine whether a breach occurred or demonstrate that there is a low probability that the PHI has been compromised based upon the following:

3.2.2. A preliminary risk assessment is conducted considering the following factors.

3.2.2.1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification.

For example, it should be considered whether the PHI included particularly sensitive financial information such as social security or credit card numbers. The nature and degree of any clinical information used or disclosed should also be considered.

3.2.2.2 The identity of the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made.

For example, it should be considered whether the person using or receiving the PHI has independent obligations to protect the privacy and security of the information. Although all CEs (Covered Entity) are obligated to protect PHI, an impermissible disclosure from one CE to another (unless it meets a statutory exception) does not automatically

eliminate notification requirements. However, this may be considered as one factor in the risk assessment concerning such a disclosure.

3.2.2.3 Whether the PHI was actually acquired or viewed, or whether only the opportunity to do so existed.

For example, if a CE mails PHI concerning a patient to the wrong address, but the envelope is returned unopened, this may pose a different risk than if the CE receives a phone call from a recipient who has reviewed the PHI and realized it was sent in error.

3.2.2.4. The extent to which the risk to the PHI has been mitigated.

For example, the recipient of an impermissible disclosure may be asked to provide assurances that the PHI will not be further used or disclosed or will be destroyed. The extent and efficacy of any such mitigation must be considered when determining the probability that the PHI has been compromised. Assurances of an employee, affiliated entity, BA or another CE, for example, may be stronger evidence of mitigation, while assurances from certain third parties may or may not be sufficient.

3.2.2.5. The Privacy Officer shall inform Executive Leadership of breaches where there is more than a low probability that the PHI has been compromised.

3.3. The Privacy Officer shall maintain a log of each suspected breach.

3.3.1. The log shall include a description of the information that may have been breached, the persons involved, whether the suspected breach is reportable, and the date of any required notifications.

3.4. If the suspected breach is determined to not be a reportable breach but nevertheless violates HIPAA or these policies, it shall be referred to the breaching party's supervisor or HR for corrective action, training, and further safeguards.

3.5. Privacy Officer shall immediately consult with the Attorney General when a suspected breach may involve 500 or more individuals.

4. Notification of Breach

4.1. The number of individuals affected by the breach determines when the notification must be submitted to the Secretary and to the patient or personal representative. (45 CFR 164.408).

4.1.1. The patient, their personal representative, or next of kin (if patient is deceased) will be notified within 60 calendar days after the date of discovery.

4.1.1.1. Notification will be the same as it is to the patient or personal representative.

4.1.2. Notification will be written in plain language, delivered first class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically and include:

4.1.2.1. A brief description of what happened, including the date of the breach, the date of the discovery of the breach, if known;

4.1.2.2. A description of the types of protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

4.1.2.3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4.1.2.4. A brief description of what USH is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

4.1.2.5. Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, an e- mail address, Web site, or postal address.

4.1.3. In cases where there is insufficient or out-of-date contact information for individuals, then such substitute notice may be provided by an alternative following CFR 164.404.

4.2. Notification of US Secretary of Health and Human Services

4.2.1. In addition to notifying affected individuals and the media (where appropriate), USH must notify the Secretary of breaches of unsecured protected health information. USH will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form.

4.2.1.1. If a breach affects 500 or more individuals, USH must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, USH may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred. (45 CFR 164.408).

4.2.1.1.1. This notice must be submitted electronically by completing all information required on the breach notification form. A separate form must be completed for every breach that has occurred during the calendar year.

4.2.1.1.2. If USH has submitted a breach notification form to the Secretary discovers additional information to report, USH may submit an additional form, checking the appropriate box to signal that it is an updated submission.

4.3. Notification to Media

4.3.1. If a breach affecting more than 500 individuals, in addition to notifying the affected individuals, USH is required to provide notice to prominent media outlets serving the State or jurisdiction.

4.3.2. USH will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area.

4.3.3. This media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

4.4. Notification by a Business Associate

4.4.1. If a breach of unsecured protected health information occurs at or by a business associate or their subcontractor, the business associate must notify USH following the discovery of the breach within one business day. The business associate must notify USH within one business day of the discovery of a suspected intentional or accidental breach of unsecured protected health information.

4.4.2. To the extent possible, the business associate should provide the covered entity with identification of each individual reasonably believed to be affected by the breach as well as any information required to be provided by the covered entity in it's notification to affected individuals.

4.5. Administrative Requirements and Burden of Proof

4.5.1. USH and business associates have the burden of proof to demonstrate that all required notifications have been provided or that there is a low probability that the protected health information has been compromised.

5. Retaliation is prohibited.

5.1. No member of the USH workforce will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:

5.1.1. Any individual for exercising any right established under HIPAA or the privacy policies, or for participating in any process established under the USH privacy policies;

5.1.2. Any individual for:

5.1.2.1. Filing a complaint with USH or with the United States Department of Health and Human Services;

5.1.2.2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to privacy policy; or

5.1.2.3. Opposing any unlawful act or practice, provided that:

5.1.2.3.1. The individual has a good faith belief that the act or practice being opposed is unlawful; and

5.1.2.3.2. The manner of such opposition is reasonable and does not involve a disclosure of an individual's protected health information in violation of privacy policies.

6. Disclosures by whistle-blowers and workforce crime victims.

6.1. A member of the USH workforce or a USH business associate may disclose an individual's protected health information and is not considered to have violated this policy if:

6.1.1. The USH employee or business associate believes USH has engaged in conduct that is unlawful or that otherwise violates professional/clinical standards, or USH policy, or that the care, services, or conditions provided by USH could endanger USH staff, persons in USH care, or the public; and

6.1.2. The disclosure is to:

6.1.2.1. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of USH;

6.1.2.2. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by USH; or

6.1.2.3. An attorney retained by or on behalf of the USH employee or business associate for the purpose of determining the legal options of the USH employee or business associate with regard to this policy.

6.2. A member of the USH workforce may disclose limited protected health information about an individual to a law enforcement official if the member of the workforce is the victim of a criminal act and the disclosure is:

6.2.1. About the suspected perpetrator of the criminal act; and

6.2.2. Limited to the following information about the suspected perpetrator:

6.2.2.1. Name and address;

6.2.2.2. Date and place of birth;

6.2.2.3. Social security number;

6.2.2.4. ABO blood type and *rh* factor;

6.2.2.5. Type of any injury;

6.2.2.6. Date and time of any treatment;

6.2.2.7. Date and time of death, if applicable; and

6.2.2.8. A description of distinguishing characteristics, including height, weight, gender, race, hair and eye color, presence or absence of beard or mustache, scars, and tattoos.

Implemented: 6-03
Revised: 1-05
Reviewed: 7-07
Reviewed: 5-09
Revised: 10-10
Revised: 8-13

Chapter: Medical Records (MR)
Section 13: HIPAA Minimum Necessary Information

Policy

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

Protected health information is not accessed, acquired, used or disclosed when it is not necessary for a particular function or purpose.

Procedure

1. General

    1.1. When using or disclosing protected health information, or when requesting protected health information from another covered entity, USH will make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

    1.2. The requirement for limiting uses and disclosures to the minimum necessary does not apply to:

        1.2.1. Disclosures to or requests by a health care provider for treatment;

        1.2.2. Disclosures made to the individual about his or her own protected information;

        1.2.3. Uses or disclosures authorized by the individual in writing that are within the scope of the authorization;

        1.2.4. Disclosures made to the United States Department of Health and Human Services (DHHS), Office for Civil Rights, when disclosure is required under the Privacy Rule for enforcement purposes;

        1.2.5. Uses or disclosures that are required by law; and

        1.2.6. Uses or disclosures that are required for compliance with the HIPAA Transaction Rule.

2. Minimum Necessary disclosures

    2.1. USH employees may rely on a requested disclosure as being the minimum necessary for the stated purpose when:

        2.1.1. Making disclosures that are permitted without authorization to public officials if the public official represents that the information requested is the minimum necessary for the stated purpose(s). For more information regarding disclosures without authorization refer to the Use and Disclosure of Protected Health

Information policy. A "public official" is any employee of a government agency who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency.

2.1.2. The information requested by another entity that is a "covered entity" under HIPAA..;

2.1.3. The information is requested by a professional who is a member of the workforce of the USH or is a business associate of the USH for the purpose of providing professional services to the "covered entity," if the professional represents that the information requested is the minimum necessary for the state purpose(s); or

2.1.4. The disclosure is for research purposes, and the person requesting the disclosure has provided documentation that complies with the Uses and Disclosures for Research Purposes policy.

2.2. USH is not required to rely on a requested disclosure as being the minimum necessary if such reliance does not appear reasonable under the circumstances.

3. Access and uses of information.

3.1. USH will identify the employees or classes of employees who need access to protected health information to carry out their duties.

3.2. For each person or class of persons, USH will identify the categories of protected health information to which access is needed, and identify any conditions appropriate to the access.

3.3. USH employees will only access records of those patients to whom they are currently assigned to provide care and treatment.

4. Criteria for disclosure of an individual's information.

4.1. Unless another policy more specifically applies, the USH Privacy Officer shall develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought. Requests for disclosure are reviewed on an individual basis in accordance with such criteria.

5. Requesting an individual's information from another entity.

5.1. When requesting information about an individual, employees must limit requests to those that are reasonably necessary to accomplish the purpose for which the request is made, in accordance with criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose.

5.2. USH will not use, disclose, or request an individual's entire medical record unless it is specifically justified that the entire medical record is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

Implemented: 6-03
Reviewed: 1-05
Reviewed: 7-07
Reviewed: 5-09
Revised: 10-10
Revised: 9-13

Chapter: Medical Records (MR)
Section 14: HIPAA Privacy Rights of Individuals

Policy

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

Individuals have the right to access, inspect, amend, and obtain a copy of protected health information consistent with certain limitations and may file a complaint if they feel those rights have been violated.

Procedure

1. General

1.1. Individuals have the right to:

1.1.1. Access, inspect and obtain a copy of their protected health information, consistent with certain limitations;

1.1.2. Receive a list of disclosures USH has made of their protected health information for up to six years prior to the date of the request.

1.1.3. Submit complaints if they have reason to suspect that information about them has been improperly used or disclosed, or if they have concerns about the privacy policies of USH; and

1.1.4. Be notified in writing, without unreasonable delay and in no case later than 60 calendar days after discovery, of any reportable breaches of their protected health information.

1.2. Individuals may ask USH to take specific actions regarding the use and disclosure of their protected health information and USH may either approve or deny the request. Specifically, individuals have the right to request:

1.2.1. Restrictions on the uses and disclosures of their protected health information while carrying out treatment, payment activities, or health care operations;

1.2.2. Protected health information be provided by alternate means, such as mail, e-mail, fax or telephone, or at alternate locations; and

1.2.3. Amendments to correct inaccurate or incomplete protected health information held by USH.

1.3. Notice of Privacy Practices. (45 CFR 164.520)

1.3.1. USH will use the, "Utah State Hospital Notice of Privacy Practices," to inform individuals about how USH may use and/or disclose their protected health information. The "Notice of Privacy Practices" also describes the actions an individual may take, or request USH to take, with regard to the use and/or disclosure of their protected health information.

Exception: The Utah State Hospital is not required to provide inmates confined to the Forensic Unit with a copy of the Notice. An "inmate" means a person incarcerated in or otherwise confined to a correctional institution.

When Forensic Unit inmates are released on parole, probation, supervised release, or no longer in custody, they have the same privacy rights as all other individuals.

1.3.2. The Notice will be:

1.3.2.1. Provided to all individuals or their personal representative no later than the first day of service;

Exception: In emergency treatment situations, the Notice should be provided as soon as reasonably practicable after the emergency has ended.

1.3.2.2. Prominently posted in each residential unit and in the admissions office;

1.3.2.3. Prominently posted on the USH website; and

1.3.2.4. Provided to anyone who asks for it.

1.3.3. USH will request all individuals receiving the Notice to complete the "Acknowledgment of Receipt of Notice" form. If the individual does not acknowledge receipt of the Notice, USH will document its good faith efforts to obtain it and the reason why acknowledgment was not obtained.

1.3.3.1. The "Acknowledgment of Receipt of Notice" will be filed in the individual's case record.

1.3.4. The privacy officer is responsible for ensuring the Notice is distributed, posted, and available as required.

1.4. Decision-making authority within USH.

1.4.1. Prior to any decision regarding an individual's request for access to protected health information or amendment to protected health information, the hospital superintendent, clinical director, or a designated licensed health care professional reviews the request and any related documentation. The licensed health care professional may be a USH staff person involved in the individual's care.

1.4.2. USH may deny an individual access to their protected health information on the grounds that access is reasonably likely to endanger the life and physical safety of the individual or another person. USH will not deny access merely on the

basis of the sensitivity of the health information or the potential for causing emotional or psychological harm. However, prior to any decision to deny such access, the hospital clinical director, or a licensed health care professional designated by the clinical director or superintendent, reviews the request and any related documentation. The licensed health care professional may be a USH staff person involved in the individual's care.

Policy

2. Rights to request privacy protection of protected health information. (45 CFR 164.522)

    2.1. Individuals have the right to request restrictions on the use and/or disclosure of their protected health information.

Procedure

1. Requesting restrictions of uses and disclosures.

    1.1. Individuals may request that USH restrict the use and/or disclosure of their protected health information for:

        1.1.1. Carrying out treatment, payment, or health care operations;

        1.1.2. Disclosing protected health information to a relative or other person who is involved in the individual's care.

    1.2. All requests for restrictions will be made by having the individual complete a "Restriction of Use and Disclosures Request Form."

    1.3. USH is not required to agree to a restriction requested by the individual.

        1.3.1. USH will not agree to restrict uses or disclosures of information if the restriction would adversely affect the quality of the individual's care or services.

        1.3.2. USH cannot agree to a restriction that would limit or prevent USH from making or obtaining payment for services.

Exception: Federal regulations 42 CFR Part 2 prohibit USH from denying a request for restrictions on uses and disclosures of an individual's information regarding alcohol and drug treatment.

    1.4. USH will document the individual's request for restrictions, and the reasons for granting or denying the request in the individual's case file.

        1.4.1. Prior to any use or disclosure of protected health information, USH staff must confirm that such use or disclosure has not been granted a restriction by reviewing the individual's case file.

    1.5. If USH agrees to an individual's request for restriction, USH will not use or disclose information that violates the restriction.

Exception: If the individual needs emergency treatment and the restricted information is needed to provide emergency treatment, USH may use or disclose such information to the extent needed to provide the emergency treatment. USH requests that the emergency treatment provider not to use or disclose the protected health information further.

1.6. USH may terminate its agreement to a restriction if:

1.6.1. The individual agrees to or requests termination of the restriction in writing;

1.6.2. The individual orally agrees to, or requests, termination of the restriction. USH will document the oral agreement or request in the individual's USH case file; or

1.6.3. USH informs the individual in writing that USH is terminating its agreement to the restriction. Information created or received while the restriction was in effect shall remain subject to the restriction.

Policy

2. Rights of individual to request to receive information from USH by alternate means or at alternate locations.

3.1. USH must accommodate reasonable requests by individuals to receive communications by alternate means, such as by mail, e-mail, fax or telephone; and

3.2. USH must accommodate reasonable requests by individuals to receive communications at an alternate location.

Procedure

1. Requesting alternate means or locations. (45 CFR 164.522)

1.1. The individual must specify the preferred alternate means or location.

1.2. Requests for alternate means or alternate locations for information may be made orally or in writing.

1.3. If an individual makes a request orally, USH will document the request and ask for the individual's signature.

1.4. If an individual makes a request by telephone or electronically, USH will document the request and verify the identity of the requester.

1.5. Prior to sending any protected health information to the individual, USH staff must confirm if the individual has requested an alternate location or by alternate means, and if USH has granted that request, by reviewing the individual's case file.

Policy

4. Rights of individuals to access protected health information. (45 CFR 164.524)

4.1. Individuals have the right to access, inspect, and obtain a copy of their protected health information maintained in a USH designated record set, except as described in Subsection 4.1.1.2 below.

4.1.1. If USH maintains information about the individual in a record that includes information about other people, the individual is only authorized to see information about him or herself, except as provided below:

4.1.1.1. A minor's parent or legal guardian may obtain protected health information without the minor's authorization about a minor if authorized under Utah law. Parent or legal guardian may not have access to the minor's protected health information when the minor is emancipated or married, when a female minor seeks treatment in connection with her pregnancy or child birth, when a minor seeks treatment for a sexually transmitted disease, or when a court has given the minor the legal right to consent.

4.1.1.2. A guardian or legal custodian may obtain protected health information about an adult if the guardian or legal custodian is authorized by Utah law to have access to the adult's information or to act on behalf of the adult for making decisions about the adult's services or care.

4.1.1.3. Agencies established to advocate and protect the rights of individuals with developmental disabilities under part C of the Developmental Disabilities Assistance and Bill of Rights Act (42 U.S.C. 6041 et seq.) and the rights of individuals with mental illness under the Protection and Advocacy for Individuals with Mental Illness Act (42 U.S.C. 10801 et seq.), shall have access to the records of their clients who have authorized access.

4.1.1.4. To obtain records of a deceased individual a person must be the legally authorized representative of the deceased individual. Heath records of an individual who has been deceased for more than fifty years are no longer protected by HIPAA, however, access to the deceased individual's records are then regulated by GRAMA. An "Access to Deceased Individual's Records Request Form" must be submitted with documentation attached identifying that requesting person has authority to act on behalf of the deceased individual or of the individual's estate.

4.2. Individuals do not have the right to access the following types of protected health information:

4.2.1. Psychotherapy notes;

4.2.2. Information compiled for use in civil, criminal, or administrative proceedings;

Exception: In accordance with UCA 62A-15-643, the individual has the right to access all certificates, applications, records, and reports prepared for the involuntary commitment proceedings.

4.2.3. Information that is subject to or exempt from the federal Clinical Laboratory Improvements Amendments of 1988.

4.2.4. Information that, in good faith, USH believes may endanger the life or physical safety of the individual or any other person.

Procedure

1. Requesting access to information.

    1.1. Individuals may request to access, inspect and obtain a copy of protected health information about themselves, subject to certain limitations.

        1.1.1. All requests for access will be made by having the individual complete the "Access to Records Request" form. The form will be received and processed by the privacy officer.

Exception: The Utah State Hospital may deny a request, in whole or in part, from a Forensic Unit inmate to obtain a copy of protected health information if obtaining a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual, other inmates or the safety of any officer, employee or other person at the Forensic Unit or responsible for transporting the inmate. However, USH must allow an inmate to inspect their protected health information unless one of the grounds for denial sited in this policy applies.

2. Timeframes to action on a request for access.

    2.1. USH must act on an individual's request for access no later than 30 days after receiving the request.

        2.1.1. In cases where the information is not maintained or accessible on-site, USH must act on the individual's request no later than 60 days after receiving the request.

        2.1.2. If USH is unable to act within these 30-day or 60-day limits, USH may extend this limitation by up to an additional 30 days, subject to the following:

            2.1.2.1. USH must notify the individual in writing of the reasons for the delay and the date by which USH will act on the request.

            2.1.2.2. USH will use only one such 30-day extension to act on a request for access.

    2.2. If USH grants the individual's request, in whole or in part, USH must inform the individual of the access decision and provide the requested access.

        2.2.1. If USH maintains the same information in more than one format (such as electronically and in a hard-copy file) or at more than one location, USH need only provide the requested protected information once.

        2.2.2. USH must provide the requested information in a form or format requested by the individual, if readily producible in that form or format. If not readily producible, USH will provide the information in a readable hard-copy format or such other format as agreed to by USH and the individual.

        2.2.3. USH may provide the individual with a summary of the requested information, in lieu of providing access, or may provide an explanation of the information if access had been provided, if:

            2.2.3.1. The individual agrees in advance; and

            2.2.3.2. The individual agrees in advance to any fees USH may impose.

2.2.4. USH must arrange with the individual for providing the requested access in a time and place convenient for the individual and USH. This may include mailing the information to the individual if the individual so requests or agrees.

2.2.5. An individual may request a copy of their protected health information or a written summary or explanation. USH will provide a copy of the requested protected health information without charge to the individual in accordance with R495-810-2, Fee Schedule for Record Copies. USH may charge a cost-based fee to prepare an explanation or summary of the requested information, if agreed to in advance by the individual.

3. Denial of access – unreviewable grounds for denial

3.1. An individual does not have the right to a review of a decision to deny access in the following circumstances:

3.1.1. The protected health information was obtained from someone other than a health care provider under a promise of confidentiality, and access would reveal the source of the information;

3.1.2. The protected health information was contained in psychotherapy notes.

3.1.3. The request to obtain a copy of protected health information would jeopardize the health, safety, security, custody, or rehabilitation of inmates at the Forensic Unit or the safety of any officer, employee, or other person at the Forensic unit or responsible for transporting an inmate;

3.1.4. The protected health information was compiled for use in civil, criminal, or administrative proceedings; or

3.1.5. The protected health information is subject to the Clinical Laboratory Improvements Amendments of 1988.

4. Denial of access - reviewable grounds for denial

4.1. An individual has the right to a review of a decision to deny access in the following circumstances:

4.1.1. Endangerment: A licensed health care professional has determined, in the exercise of professional judgment, that the information requested is reasonably likely to endanger the life or physical safety of the individual or another person; or

4.1.2. Personal Representative: The request for access is made by the individual's personal representative, and a licensed health care professional or other designated staff has determined, in the exercise of professional judgment, that allowing the personal representative to access the information is reasonably likely to cause substantial harm to the individual or to another person.

4.1.3. Reference to Another Person: The protected health information makes reference to another person, and a licensed health care professional has determined, in the exercise of professional judgment, that the information requested is reasonably likely to cause substantial harm to that person.

4.2. The individual has the right to have the decision to deny reviewed by a licensed health care professional not directly involved in making the original denial decision. USH will provide or deny access in accordance with this review.

4.2.1. The reviewer must determine, within a reasonable time, whether to approve or deny the individual's request for access.

4.2.2. USH must then:

4.2.2.1. Promptly notify the individual in writing of the reviewer's determination; and

4.2.2.2. Take action to carry out the reviewer's determination.

4.2.3. If USH denies access, in whole or in part, to the requested information, USH must:

4.2.3.1. Give the individual access to any other requested individual information, after excluding the information to which access is denied;

4.2.3.2. Provide the individual with a timely written denial. The denial must:

4.2.3.2.1. State the basis for the denial, in plain language;

4.2.3.2.2. If the reason for the denial is due to danger or harm to the individual or another, explain the individual's review rights as specified in Section 4b, Denial of Access – Reviewable Grounds for Denial of this procedure, above, including an explanation of how the individual may exercise these rights; and

4.2.3.2.3. Provide a description of how the individual may file a complaint with USH, (including the name or title and telephone number of the contact person) or with the United States Department of Health and Human Services (DHHS) Office for Civil Rights.

4.2.4. If USH does not maintain the requested protected health information, and knows where such information is maintained (such as by a medical provider, insurer, other public agency, private business, or other non USH entity), USH must inform the individual of where to direct the request for access.

Policy

5. Rights of individuals to request amendments to their information. (45 CFR 164.526)

5.1. Individuals have the right to request that USH amend their protected health information in USH designated record sets.

5.2. USH is not obligated to agree to an amendment and may deny the request or limit its agreement to amend.

Procedure

1. Requesting amendments of protected health information.

    1.1. All requests for amendments will be made by having the individual complete the, "Amendment of Health Record Request" form.

        1.1.1. Supporting documentation for request is limited to four (4) pages.

    1.2. USH must act on the individual's request no later than 60 days after receiving the request. If USH is unable to act on the request within 60 days, USH may extend this time limit by up to an additional 30 days, subject to the following:

        1.2.1. USH must notify the individual in writing of the reasons for the delay and the date by which USH will act on the receipt; and

        1.2.2. USH will use only one such 30-day extension.

    1.3. If USH grants the request, in whole or in part, USH must:

        1.3.1. Make the appropriate amendment to the protected health information in the designated record set and document the amendment in the individual's file or other designated record set;

        1.3.2. Provide timely notice to the individual that the amendment has been accepted, pursuant to the time limitations in Section 1.c. of this procedure, above;

        1.3.3. Seek the individual's agreement to notify other relevant persons or entities, with whom USH has shared, or needs to share, the amended information; and

        1.3.4. Make reasonable efforts to inform, and to provide the amendment within a reasonable time to:

            1.3.4.1. Persons named by the individual as having received protected information and who need the amendment; and

            1.3.4.2. Persons, including business associates of USH, who have the protected information that is the subject of the amendment and who may have relied, or could foreseeably rely, on the information to the individual's detriment.

        1.3.5. Prior to any decision to amend protected health information, the request and any related documentation shall be reviewed by the hospital superintendent, clinical director, a licensed health care professional designated by the superintendent, or a USH staff person involved in the individual's case.

    1.4. USH may deny the individual's request for amendment if:

        1.4.1. USH finds the information to be accurate and complete;

        1.4.2. The information was not created by USH, unless the individual provides a reasonable basis to believe that the originator of such information is no longer available to act on the requested amendment;

1.4.3. The protected health information is not part of the USH designated record set.

1.4.4. The protected health information is not available for inspection under Section 4 of this policy, Rights of Individuals to Access Protected Health Information.

1.5. If USH denies the requested amendment, in whole or in part, USH must provide the individual with a timely written denial. The denial must

1.5.1 Be sent or provided within the time limits specified in Section 1.3, of this procedure, above;

1.5.2 State the basis for the denial, in plain language;

1.5.3 Explain the individual's right to submit a written statement disagreeing with the denial. The statement is limited to four pages in length.

1.5.3.1 USH will enter the written statement into the individual's case file;

1.5.3.2 USH may prepare a written rebuttal of the individual's written statement and enter it into the individual's case file. USH will send or provide a copy of the written rebuttal to the individual;

1.5.3.3 USH will include a copy the individual's request, the denial, the statement, and the written rebuttal, with any future disclosures of the relevant information;

1.5.3.4 Explain that if the individual does not submit a written statement of disagreement, the individual may ask that if any future disclosures of the relevant information, will include a copy of the individual's original request for amendment and a copy of the USH written denial; and

1.5.3.5 Provide information on how the individual may file a complaint with USH, (including the name or title and telephone number of the contact person) or with the U.S. Department of Health and Human Services (DHHS), Office for Civil Rights.

Policy

6. Rights of individuals to an accounting of disclosures of protected health information. (45 CFR 164.528)

6.1 Individuals have the right to receive an accounting of disclosures of protected health information made by USH.

6.2 The accounting to the individual will only include health information not previously authorized by the individual for use or disclosure, and will not include information collected, used or disclosed for treatment, payment or health care operations for that individual.

6.3 This right does not apply to disclosures made prior to the effective date of this policy, which is April 14, 2003.

Procedure

1. Requesting an accounting of disclosures.

    1.1 When a individual requests an accounting of disclosures that USH has made of their protected health information (PHI), USH must provide that individual with a written accounting of such disclosures made during the six- year period (or lesser time period if specified by the requesting individual) preceding the date of the individual's request.

    1.2 All requests for an accounting of disclosures will be made by having the individual complete the "Accounting of Disclosures Request" form.

    1.3 Examples of disclosures of protected health information (PHI) that are required to be listed in an accounting (unless prohibited by federal law or restricted by the individual) include:

        1.3.1 Abuse Report: PHI provided pursuant to mandatory abuse reporting laws to an entity authorized by law to receive the abuse report.

        1.3.2 Audit Review: PHI provided in relation to an audit or review (whether financial or quality of care or other audit or review) of a provider or contractor.

        1.3.3 Business Associates: PHI disclosed to or by business associates of USH.

        1.3.4 Health and Safety: PHI provided to avert a serious threat to health or safety of a person.

        1.3.5 Licensee/Provider: PHI provided in relation to licensing or regulation or certification of a provider or licensee or entity involved in the care or services of the individual.

        1.3.6 Legal Proceeding: PHI that is ordered to be disclosed pursuant to a court order in a court case or other legal proceeding. A copy of the court order shall be provided with the accounting.

        1.3.7 Law Enforcement Official/Court Order: PHI provided to a law enforcement official pursuant to a court order. A copy of the court order shall be provided with the accounting.

        1.3.8 Law Enforcement Official/Deceased: PHI provided to law enforcement officials or medical examiners about a person who has died for the purpose of identifying the deceased person, determining cause of death, or as otherwise authorized by law.

        1.3.9 Law Enforcement Official/Warrant: PHI provided to a law enforcement official in relation to a fleeing felon or for whom a warrant for their arrest has been issued and the law enforcement official has made proper request for the information, to the extent otherwise permitted by law.

        1.3.10 Media: PHI provided to the media (TV, newspaper, etc.) that is not within the scope of an authorization by the individual.

        1.3.11 Public Health Official: PHI about an individual provided by staff to a public health official, such as the reporting of disease, injury, or the conduct of a public health study or investigation.

1.3.12 Research: PHI about an individual provided by USH staff for purposes of research conducted without authorization, using a waiver of authorization approved by an Institutional Review Board (IRB). USH shall include a copy of the research protocol with the accounting, along with the other information required under the HIPAA privacy rule, 45 CFR 164.528(b)(4).

1.4. USH is not required to provide the individual with an accounting of disclosures that are:

1.4.1. Authorized by the individual;

1.4.2. Made prior to the original effective date of this policy, which is April 14, 2003;

1.4.3. Made to carry out treatment, payment, and health care operations;

1.4.4. Made to the individual;

1.4.5. Made to persons involved in the individual's health care;

1.4.6. Made as part of a limited data set in accordance with the De-identification of Individual Information and Use of Limited Data Sets policy.

1.4.7. Made for national security or intelligence purposes; or

1.4.8. Made to correctional institutions or law enforcement officials having lawful custody of an inmate.

1.5. The accounting must include, for each disclosure:

1.5.1. The date of the disclosure;

1.5.2. The name, and address if known, of the person or entity who received the disclosed information;

1.5.3. A brief description of the information disclosed; and

1.5.4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, a copy of any request for disclosure from the Department of Health and Human Services, public health authority, court order, or authorized government authority.

1.6. If USH has made multiple disclosures to the same person or entity for the same purpose, USH need not list the same person or entity if USH adds to the first disclosure:

1.6.1. The frequency or number of disclosures made during the accounting period; and

1.6.2. The last date of the disclosure made during the requested time period.

1.7. USH must act on the individual's request for an accounting no later than 60 days after receiving the request, subject to the following:

1.7.1. If unable to provide the accounting within 60 days after receiving the request, USH may extend this requirement by another 30 days. USH must provide the individual with a written statement of the reasons for the delay within the original

60-day limit, and inform the individual of the date by which USH will provide the accounting.

1.7.2. USH will use only one such 30-day extension.

1.8. USH must provide the first requested accounting in any 12-month period without charge. USH may charge the individual a reasonable cost-based fee for each additional accounting requested by the individual within the 12-month period following the first request, provided that USH:

1.8.1. Informs the individual of the fee before proceeding with any such additional request; and

1.8.2. Allows the individual an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

1.9. USH must document, and retain in the individual's case file, the information required to be included in an accounting of disclosures and provide a copy of the written accounting to the individual.

1.10. USH will temporarily suspend a individual's right to receive an accounting of disclosures that USH has made to a health oversight agency or to a law enforcement official, for a length of time specified by such agency or official, if:

1.10.1 The agency or official provides a written statement that the accounting would likely impede their activities.

1.10.2 However, if such agency or official makes an oral request, USH will:

1.10.2.1 Document the oral request, including the identity of the agency or official making the request;

1.10.2.2 Temporarily suspend the individual's right to an accounting of disclosures pursuant to the request; and

1.10.2.3 Limit the temporary suspension to no longer than 30 days from the date of the oral request, unless the agency or official submits a written request specifying a longer time period.

Policy

7. Rights of individuals to file complaints regarding use or disclosure of protected health information.

7.1. Individuals have a right to submit a complaint if they believe that USH has improperly used or disclosed their protected health information, or if they have concerns about the privacy policies of USH or concerns about USH compliance with such policies.

Procedure

1. Filing a Complaint.

1.1. Individuals may file complaints with USH, or with the U.S. Department of Health and Human Services (DHHS) - the Office for Civil Rights.

Privacy Officer **Utah State Hospital** P.O. Box 270 Provo, UT 84603-0270 Phone: (801) 344-4319 Fax: (801) 344-4223
Region VIII, Office for Civil Rights **U. S. Department of Health and Human Services** 1961 Stout Street, Room 1185 FOB Denver, CO 80294-3538 Phone: (303) 844-2024 Fax: (303) 844-2025 TDD: (303) 844-3439 Email: OCRComplaint@hhs.gov

1.2. USH will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.

1.3. USH may not require individuals to waive their rights to file a complaint as a condition of providing of treatment, payment, and enrollment in a health plan, or eligibility for benefits.

1.4. USH will document all complaints, the findings from reviewing each complaint, and USH actions resulting from the complaint. The documentation for each specific complaint will include a description of corrective actions taken, or a description of why corrective actions were not needed.

Implemented: 6-03
Revised: 1-05
Reviewed: 7-07
Revised: 10-10
Revised: 9-13

Chapter: Medical Records (MR)
Section 15: HIPAA Uses and Disclosures for Research

Policy

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

Procedure

1. Access, acquisition, use and disclosure for research purposes.

USH may access, acquire, use or disclose protected health information for research purposes with the individual's specific written authorization.

1.1.1 An authorization, must meet all the requirements described in the "Uses and Disclosures of Protected Health Information" policy, and may indicate as an expiration date such terms as "end of research study," or similar language.

1.1.2 An authorization for access, use and disclosure for a research study may be combined with any other type of written permission for the same research study, including consent to participate in the research study.

1.1.3 The researcher may condition research related treatment on the provision of an authorization for access, use and disclosure of protected health information.

1.2 USH may use or disclose protected health information for research purposes without the individual's written authorization provided that:

1.2.1 USH obtains documentation that a waiver of an individual's authorization for release of protected health information has been approved by the Utah Department of Human Services IRB.

1.2.1.1 If DHS IRB declines, in writing, to review the research proposal, USH obtains documentation that a waiver of an individual's authorization for release of protected health information has been approved by either a non-DHS IRB, or

1.2.1.2 A Privacy Board that:

1.2.1.2.1 Has members with varying backgrounds and appropriate professional competency as needed to review the effect of the research protocol on the individual's privacy rights and related interests;

1.2.1.2.2 Includes at least one member who is not affiliated with USH, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entity; and

1.2.1.2.3 Does not have any member participating in a review of any project in which the member has a conflict of interest.

1.2.2. Documentation required of the IRB or privacy board when granting approval of a waiver of authorization must include:

1.2.2.1. A statement identifying the IRB or privacy board that approved the waiver of authorization, and the date of such approval;

1.2.2.2. A statement that the IRB or privacy board has determined that the waiver of authorization, in whole or in part, satisfies the following criteria:

1.2.2.2.1. The access, acquisition, use or disclosure of an individual's protected health information involves no more than a minimal risk to the privacy of individuals, based on at least the following elements:

1.2.2.2.1.1. An adequate plan to protect an individual's identifying information from improper access, acquisition, use or disclosure;

1.2.2.2.1.2. An adequate plan to destroy an individual's identifying information at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the information or such retention is otherwise required by law; and

1.2.2.2.1.3. Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the access, acquisition, use or disclosure of the protected health information would be permitted under this policy;

1.2.2.2.2. The research could not practicably be conducted without the waiver; and

1.2.2.2.3. The research could not practicably be conducted without access to and use of the individual's protected health information.

1.2.2.3. A brief description of the protected health information for which access, acquisition, use or disclosure has been determined to be necessary by the IRB or privacy board;

1.2.2.4. A statement that the waiver of an individual's authorization has been reviewed and approved under either normal or expedited review procedures, by either an IRB or a privacy board, pursuant to 45 CFR 164.512(i)(2)(iv); and

1.2.2.5. A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who is not affiliated with the USH, not affiliated with the entity conducting or sponsoring the research, and not related to any person affiliated with USH, or the entity conducting or sponsoring the research. The waiver of authorization must be approved by the majority of the privacy board members present at the meeting.

1.2.2.6. The privacy board may elect to use an expedited review procedure if the research involves no more than minimal risk to the privacy of individuals. The review and approval of the waiver of authorization may be carried out by the chair of the privacy board or by a member designated by the chair.

1.2.2.7. The documentation of the waiver must be signed by the chair of the IRB or privacy board or by a member designated by the chair.

1.2.3. A researcher may request access to individual protected health information maintained by USH in preparation for research. USH will only provide such access if USH obtains, from the researcher, written representations that:

1.2.3.1 Use or disclosure is sought solely to review an individual's protected health information to prepare a research protocol or for similar purposes to prepare for the research project;

1.2.3.2 No protected health information will be removed from USH by the researcher in the course of the review; and

1.2.3.3 The protected health information for which use or access is sought is necessary for the research purposes;

1.2.4. USH may provide access if USH obtains the following from the researcher:

1.2.4.1 Representation that the access, acquisition, use or disclosure is sought solely for research on the protected health information of deceased persons;

1.2.4.2 Documentation, if USH requests, of the death of such persons; and

1.2.4.3 Representation that the individual's protected health information for which use or disclosure is sought is necessary for the research purposes.

Implemented: 6-03
Reviewed: 1-05
Reviewed: 7-07
Reviewed: 5-09
Revised: 10-10
Revised: 9-13

Chapter: Medical Records (MR)
Section 16: HIPAA Administrative Requirements

Policy

USH acquires, creates, accesses, uses, discloses, maintains, transmits and destroys protected health information in accordance with the "Health Insurance Portability Act of 1996" (HIPAA), 45 CFR 160, 162, and 164, as amended by the "American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act" (HITECH) and the Omnibus Rule.

Procedure

1. Privacy Officer

    1.1. USH privacy officer is responsible for:

        1.1.1. Developing and implementing the USH privacy policies and procedures;

        1.1.2. Receiving, documenting, tracking, and investigating all complaints regarding the privacy policies, procedures, and suspected breaches of PHI;

            1.1.2.1. The privacy officer maintains a breach log.

            1.1.2.2. The privacy officer ensures notification and reporting requirements for breaches are completed.

        1.1.3. Providing further information about matters covered by the Notice of Privacy Practices;

        1.1.4. Providing training on the privacy policies and procedures to all members of the USH workforce (employees, volunteers, interns, and others under the direction of USH);

        1.1.5. Establishing and maintaining a system to account for disclosures of protected health information;

        1.1.6. Developing and maintaining the designated record set; and

        1.1.7. Initiating, facilitating and promoting activities to foster awareness of the privacy polices and procedures within the USH.

    1.2. USH documents the designation of the privacy officer in accordance with the Documentation Requirements, Subsection 5, of this policy.

2. Changes to Policies and Procedures

    2.1. USH changes its policies and procedures when necessary to comply with changes in state and federal law.

2.2. If the change in law materially affects the contents of the Notice of Privacy Practices, USH must promptly make the appropriate revisions to the notice and comply with the change in law.

2.3. USH may make changes to polices and procedures not reflected in the Notice of Privacy Practices at any time, provided that both of the following conditions are met:

2.3.1. The changes comply with the HIPAA Privacy Rule; and

2.3.2. Before the effective date of the change, the changes are documented in accordance with the Documentation Requirements, Subsection 5, of this policy.

3. Changes to Notice of Privacy Practices

3.1. USH will promptly revise and post the Notice of Privacy Practices whenever there is a change to the uses and disclosures, the individual's rights, the USH legal duties, or other privacy practices. USH may not implement the changes prior to the effective date of the revised Notice.

4. Training the Workforce

4.1. USH provides training on the privacy policies and procedures to:

4.1.1. Each new member of the workforce within a reasonable period of time after the person joins the workforce;

4.1.2. Each member of the workforce whose functions are affected by a material change in the privacy polices and procedures, within a reasonable period of time after the change becomes effective;

4.1.3. USH documents that training has been provided in accordance with the Documentation Requirements, subsection 5, of this policy.

5. Documentation Requirements

5.1. USH maintains its privacy polices and procedures in written form.

5.2. If the privacy policies and procedures require a communication to be in writing, USH must maintain a written or electronic copy as documentation.

5.3. If the privacy policies and procedures require an action, activity, or designation to be documented, USH maintains a written record of the action, activity, or designation.

5.4. USH retains any documentation that is required by the HIPAA Privacy Rule for six years from the date it was created, or from the date it was last in effect, whichever is later.

5.5. All documentation that is required by the privacy policies and procedures may be on paper or in electronic form.

6. DHS contracts with the Utah Department of Technology Services (DTS) to provide all of it's technological services including but not limited to compliance with the security rule and designation of Security Officer in accordance with the terms of the Business Associate Agreement.

Implemented: 6-03
Reviewed: 1-05
Reviewed: 7-07
Reviewed: 5-09
Revised: 4-10
Revised 10-10
Revised: 9-13